EXPT: 7 NMAP TO DISCOVER LIVE HOSTS USING ARP SCAN AND TCP/UDP PING SCAN

Introduction:

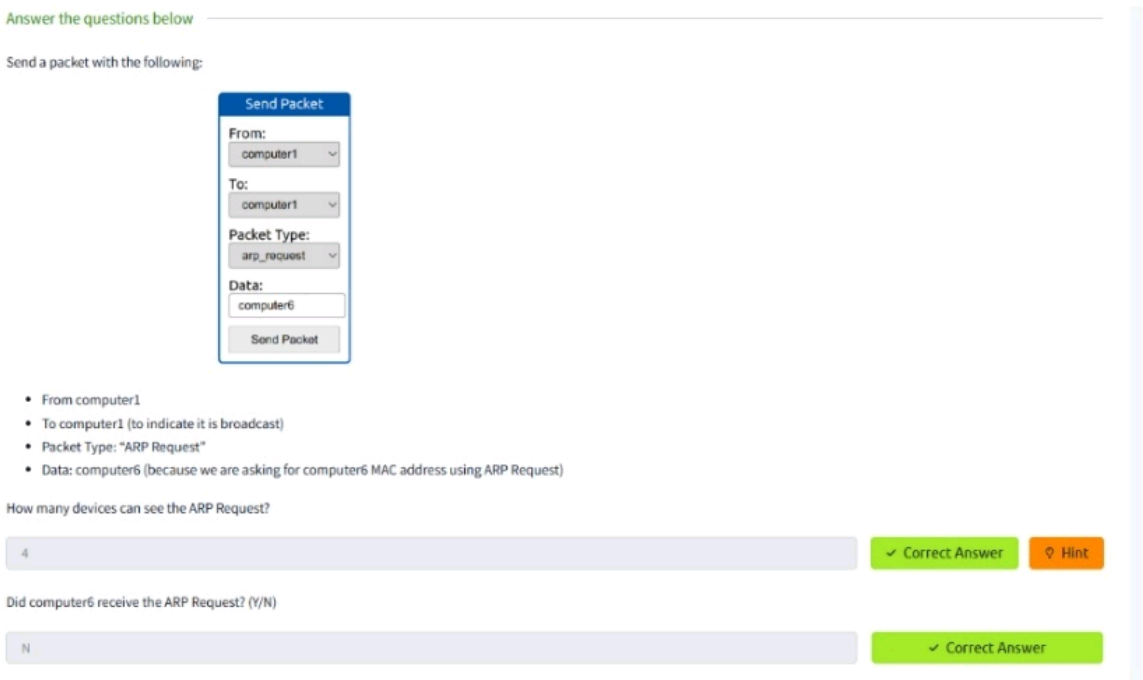
Discovering live hosts is the first step in network enumeration. Different techniques find hosts in different situations: **ARP scan** discovers machines on the same Ethernet/LAN by asking " who has this IP?" , **ICMP scan** (Ping) asks hosts to respond to ICMP Echo Requests, and a **tcpdump ping-style capture** records the actual probe and reply packets on the network so you can verify what' s sent and received. Combining these methods gives a fuller picture because some hosts

block ICMP or TCP probes but still respond to ARP, and packet capture shows the raw traffic for troubleshooting and proof.

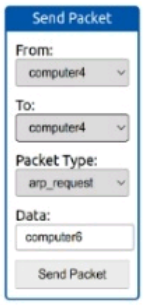
Aim:

- Use ARP scanning to detect live hosts on the local subnet.
- Use ICMP (ping) scanning to discover hosts that reply to echo requests.
- Use tcpdump to capture and inspect the probe and reply packets for verification.
- Compare results and explain why a host may appear in one scan but not another.

Tasks:



Send a packet with the following:



- From computer4
- To computer4 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: computer6 (because we are asking for computer6 MAC address using ARP Request)

How many devices can see the ARP Request?

4 ✓ Correct Answer 💡 Hint

Did computer6 reply to the ARP Request? (Y/N)

Y ✓ Correct Answer

Answer the questions below

What is the first IP address Nmap would scan if you provided `10.10.12.13/29` as your target?

10.10.12.8 ✓ Correct Answer 💡 Hint

How many IP addresses will Nmap scan if you provide the following range `10.10.0-255.101-125`?

6400 ✓ Correct Answer 💡 Hint

Send a packet with the following:

- From computer1
- To computer3
- Packet Type: "Ping Request"

What is the type of packet that computer1 sent before the ping?

ARP Request ✓ Correct Answer

What is the type of packet that computer1 received before being able to send the ping?

ARP Response ✓ Correct Answer

How many computers responded to the ping request?

1 ✓ Correct Answer

Send a packet with the following:

- From computer2
- To computer5
- Packet Type: "Ping Request"

What is the name of the first device that responded to the first ARP Request?

router ✓ Correct Answer

What is the name of the first device that responded to the second ARP Request?

computer5 ✓ Correct Answer

Send another Ping Request. Did it require new ARP Requests? (Y/N)

N ✓ Correct Answer

Answer the questions below

We will be sending broadcast ARP Requests packets with the following options:

- From computer1
- To computer1 (to indicate it is broadcast)
- Packet Type: "ARP Request"
- Data: try all the possible eight devices (other than computer1) in the network: computer2, computer3, computer4, computer5, computer6, switch1, switch2, and router.

How many devices are you able to discover using ARP requests?

3 ✓ Correct Answer

Answer the questions below

What is the option required to tell Nmap to use ICMP Timestamp to discover live hosts?

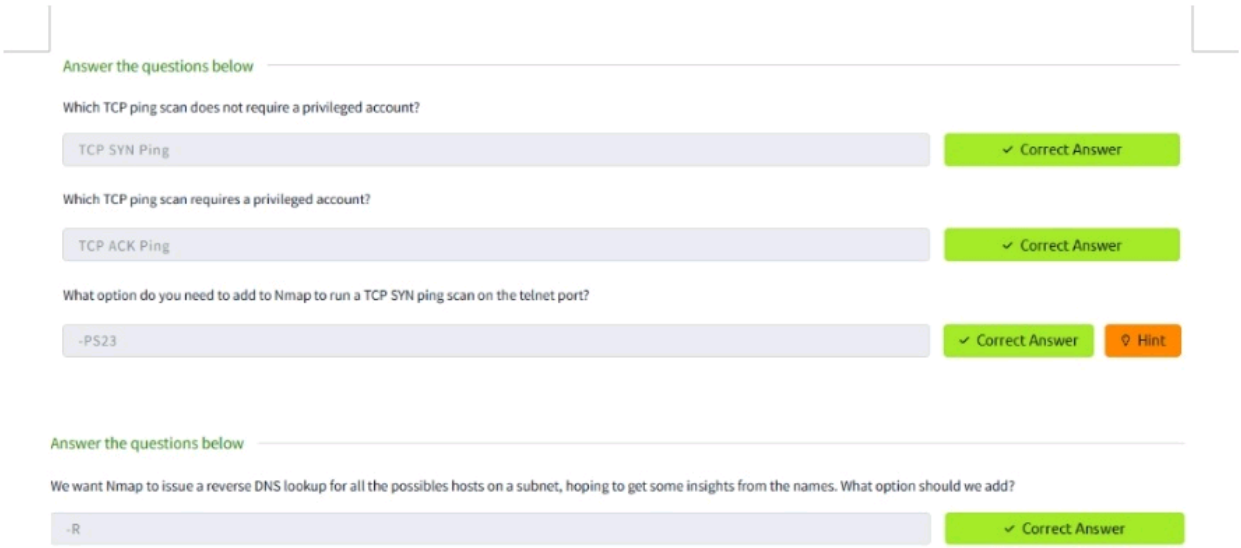
-PP ✓ Correct Answer

What is the option required to tell Nmap to use ICMP Address Mask to discover live hosts?

-PM ✓ Correct Answer

What is the option required to tell Nmap to use ICMP Echo to discover live hosts?

-PE ✓ Correct Answer



Result:

Ran an ARP scan on the local network (e.g. arp-scan or nmap -PR) and noted responsive IPs/MACs.

Performed an ICMP ping-scan (e.g. nmap -PE or fping) and recorded which hosts replied.

Started tcpdump during the ping scan to capture ICMP Echo Requests/Replies (and ARP requests/replies) for later inspection.

Performed an ICMP ping-scan (e.g. nmap -PE or fping) and recorded which hosts replied.